House Study Bill 15 - Introduced

HOUSE FILE _____
BY (PROPOSED COMMITTEE ON ECONOMIC GROWTH AND TECHNOLOGY BILL BY CHAIRPERSON SORENSEN)

A BILL FOR

An Act creating a cybersecurity unit within the office of the chief information officer.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. Section 8B.4, Code 2023, is amended by adding the following new subsection:

NEW SUBSECTION. 18A. Administer the cybersecurity unit established in section 8B.34.

Sec. 2. NEW SECTION. **8B.34 Cybersecurity unit.**

1. As used in this section, unless the context otherwise requires, *"cybersecurity incident"* means a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or cybersecurity practices.

2. A cybersecurity unit is created for the purpose of monitoring, managing, coordinating, and reporting cybersecurity incidents occurring within the state or a political subdivision of the state within the office of the chief information officer. The unit shall be administered by the chief information officer as provided in section 8B.4.

3. On or before December 31 of each year, and when requested by the general assembly, the cybersecurity unit shall provide a report to members of the general assembly containing the number and nature of incidents reported to the unit during the preceding calendar year or since the most recent report and making recommendations to the general assembly regarding cybersecurity standards for the state. If a request is made by the general assembly, a report shall be provided within thirty days of receipt of the request.

4. Qualified cybersecurity incidents shall be reported by a state agency or political subdivision to the cybersecurity unit no later than ten days following a determination that the state or political subdivision of the state experienced a qualified cybersecurity incident. A qualified cybersecurity incident shall meet at least one of the following criteria:

a. A state or federal law requires the reporting of the incident to regulatory or law enforcement agencies or affected citizens.

b. The ability of the state or political subdivision that experienced the incident to conduct business is substantially

affected.

c. The incident would be classified as emergency, severe, or high risk by the U.S. cybersecurity and infrastructure security agency.

5. The report of the cybersecurity incident to the cybersecurity unit shall include:

a. The approximate date of the incident.

b. The date the incident was discovered.

c. The nature of any data that may have been illegally obtained or accessed.

d. A list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom a notification has been or will be provided by the state agency or political subdivision.

e. Additional information to the extent available.

6. The unit shall make available information regarding recent or ongoing qualified cybersecurity incidents to political subdivisions of the state and businesses operating in the state. The information shall include:

a. The nature of the cybersecurity attack.

b. The actor or actors perpetrating the cybersecurity attack.

c. Other relevant details that would assist a political subdivision or business in addressing or securing their systems against cybersecurity attacks.

7. Procedures for reporting a cybersecurity incident shall be established by the office by rule, made available on the office's internet site, and distributed to the state and political subdivisions of the state.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill creates a cybersecurity unit under the office of the chief information officer. The office shall be administered by the chief information officer.

The bill defines "cybersecurity incident" to mean a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or cybersecurity practices.

The bill provides that the cybersecurity unit shall be responsible for managing and coordinating cyber and computer security for the state and political subdivisions of the state. Annually or at the request of the general assembly, the unit will provide a report including the number of cybersecurity incidents since the last report and updated recommendations for cybersecurity practices. If a request is made by the general assembly, the unit shall provide a report within 30 days of the receipt of the request.

The bill provides a reporting mechanism and criteria for the state or political subdivisions of the state to inform the cybersecurity unit of cybersecurity incidents. Cybersecurity incidents shall be reported to the office no later than 10 days following an incident. The bill provides that the office shall provide information to political subdivisions or businesses operating in the state regarding cybersecurity incidents. The information shall include the nature of the cybersecurity attack, the actors perpetrating the attack, and other relevant information businesses or political subdivisions should be aware of to protect information systems. The office shall establish reporting procedures required by rule and distribute the procedures to the state and political subdivisions of the state.